Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Amendment of Part 0, 1, 2, 15 and 18 of the	)	ET Docket No. 15-170
Commission's Rules regarding Authorization	)	
of Radio frequency Equipment	)	
	)	
Request for the Allowance of Optional	)	RM-11673
Electronic Labeling for Wireless Devices	)	

Comment on Proposed Rules Regarding
Mandating Software Controls Designed to Limit
Third-Party and End-User Modification of RF Equipment
of
Andy Sayler, Matt Monaco, and Dirk Grunwald

1. Introduction

We are networking and security researchers and OpenWRT users. We respectfully submit this comment in response to the proposed amendments to the rules governing the evaluation and approval of RF devices outlined in the Commission's July 21st, 2015 Notice of Proposed Rulemaking.[1] Among the changes the Commission proposes are a number of rules aimed at limiting the ability of third parties and end-users to make software modifications to RF devices that might allow modes of operation beyond those originally approved.[2] These rules replace and expand previous rules governing third party modification of Software-Defined Radio (SDR) devices.[3]

[1] Amendment of Parts 0, 1, 2, 15 and 18 of the Commission's Rules Regarding Authorization of Radio frequency Equipment, ET Docket No. 15-170, Notice of Proposed Rulemaking, 30 FCC Rcd 7725 (2015).
[2] NPRM, Paragraphs 20, 22, 45, 46, and 72.
[3] 47 CFR § 2.944; Software Freedom Law Center, *FCC Rules on FOSS and Software-Defined Radio*, July 6th, 2007.

While ensuring that RF devices are not operated in unapproved ways is an important issue for the Commission to address, doing so in a manner that places limits on the ability of end-users to modify or update the software in their RF-capable devices is likely to cause more problems than it will solve. Such rules will detrimentally affect the security of many Internet-connected systems, will limit engineering innovation, and will run counter to many of the Commission's stated goals regarding competition and user choice. Furthermore, such limitations are unlikely to be effective in practice, failing to solve the kinds of interference issues the Commission appears to be targeting via the new rules.

Instead of implementing the rules as proposed, the Commission should instead pursue solutions that do not place undue burdens on the ability of end-users to freely control the software running on their RF-enabled devices. Such solutions might include:

+ Working closely with the communities who build and maintain such software to support existing efforts to ensure regulatory compliance.
+ Educating end-users on their responsibilities when using RF-enabled devices with an aim toward ensuring regulatory compliance.
+ Stepping up enforcement against bad actors who are intentionally supplying or operating RF-enabled devices that cause harmful interference.

2. The rules as proposed will cause more harm than good.

The rules as currently proposed raise two main concerns. First, the rules will likely cause a number of unintended harms by restricting what software users may run on their devices. Second, the rules will likely be ineffective in preventing any harmful interference that might be caused by the modification of device software.

A. Restricting the ability of end-users to modify the software on their devices will introduce a number of unintended harms.

Unfortunately, the rules the Commission proposes will likely lead to it being more difficult for end-users to control the software installed on their devices. Even if the Commission intends manufactures to narrowly read the rules as only requiring restrictions on the modification of the RF-related capabilities of a device, such restrictions will likely be implemented as a general-purpose limit on all firmware modification as a matter of practicality or cost.[4] Today, end-users of RF-enabled devices (e.g. WiFi routers, cell phones, laptops, etc) derive a number a benefits from being able to replace manufacture-provided firmware with alternative firmware such as that provided by the OpenWRT project.[5] Such benefits include the ability to review publicly available source code in order to verify the security and behavior of RF-enabled devices; guaranteed access to timely updates, security patches, and enhancements; support for advanced network and protocol features (e.g. WPA Enterprise, VLANs, IPv6, DNSSEC, etc); and the ability to run experimental code in support of engineering research and development efforts. The proposed rules will unintentionally deprive end-users of these benefits.

Many of these benefits are becoming increasingly critical to ensuring the security of individual end-users and the Internet as a whole. Manufacturer-provided firmware approved to run on devices such as routers and cell phones has a history of serious security flaws.[6] Prominent security researchers have described such systems as highly vulnerable

---

[4] Comments of Harold Feld as quoted via Karl Bode, *No, The FCC Is Not (Intentionally) Trying To Kill Third-Party Wi-Fi Router Firmware,* Techdirt, September 3rd, 2015.
[5] OpenWRT: Wireless Freedom, https://openwrt.org/.
[6] Dan Goodin, *A billion Android phones are vulnerable to new Stagefright bugs,* Ars Technica, October 1st, 2015; Dan Goodin, *How hackers can access iPhone contacts and photos without*

critical infrastructure points — the subversion of which could "probably take down the Internet".[7] Unfortunately, manufactures are often slow to fix such issues once discovered, or often don't fix such issues at all.[8] If the Commission passes rules that restrict end-users' ability to install and use third party firmware, individual security as well as the security of the wider Internet will suffer.

The proposed rules will likely cause a number of additional unintended harms. For example, the GPLv3, a Free Software license that governs the use a large body of Free software and Free software libraries, specifically stipulates that the manufacturer of any product including GPLv3 licensed code must provide the end-user with the "authorization keys, or other information required to install and execute modified versions of a covered work in that user product."[9] Since complying with this licensing requirement runs directly counter to the Commission's mandate for manufacturers to specifically prohibit end-users from running modified code on their hardware, this will likely preclude the use of any GPLv3 code in RF-enabled devices. The proposed rules will thus unnecessarily make a large body of otherwise useful and valuable software unavailable to the developers and users of RF-enabled devices.

---

a password, Ars Technica, September 25th, 2015; Peter Bright, *Millions of routers vulnerable to new version of old attack,* Ars Technica, July 18th, 2015; Peter Bright, *'90s-style security flaw puts "millions" of routers at risk,* Ars Technica, May 20th, 2015; Dan Goodin, *12 million home and business routers vulnerable to critical hijacking hack,* Ars Technica, December 18th, 2014; Dan Goodin, *Hackers hijack 300,000-plus wireless routers, make malicious changes,* Ars Technica, March 3rd, 2014.

[7] Comments of Dan Geer as quoted via Sean Gallagher, *Security expert calls home routers a clear and present danger,* Ars Technica, August 6th , 2014.

[8] Dan Goodin, *No patch for remote code-execution bug in D-Link and Trendnet routers,* Ars Technica, April 28th 2015.

[9] GNU General Public License: Version 3, June 29th, 2007.

B. The proposed rules are unlikely to solve the problem of unauthorized interference due to end-user modification.

The Commission's rules seem premised on the assumption that it is technologically feasible to prevent end-user modification to the software that runs on RF-enabled devices. This capability, however, is far from guaranteed. Most previous efforts aimed at achieving a similar level of control over the software on end-user devices have failed. For example, many cell phones sold today are similarly "locked" against end-user modification, but such locks are routinely bypassed by end-users who "root" or "jailbreak" their phones.[10] Indeed, Congress passed a law in 2014 specifically allowing such practices and removing ambiguity as to their legality under the Digital Millennium Copyright Act.[11]

The Section 1201 triennial proceedings currently underway at the Copyright Office also provides numerous examples of the ineffectiveness of technological protection measures (TPMs) aimed at controlling what end-users can do with their software and devices.[12] In addition, the record in those proceedings provides numerous arguments as to the security, competition, and innovation benefits of allowing end-users the ability to study and modify such software. In fact, Section 1201's very existence is a testament to the ineffectiveness of software locks and controls — after all, if such mechanisms were effective in preventing users from modifying their devices, it would be unnecessary to have specific laws governing the ability of users to bypass them.

---

[10] Whitson Gordon, *Everything you need to know about rooting your Android phone*, Lifehacker, September 4th, 2013; *How to jailbreak iPhone, iPad, and iPod Touch*, iPhone Hacks, accessed on October 8th, 2015, http://www.iphonehacks.com/jailbreak.

[11] 17 USC § 1201

[12] United States Copyright Office, *Section 1201 Exemptions to Prohibition Against Circumvention of Technological Measures Protecting Copyrighted Works*, accessed on October 8th, 2015, http://www.copyright.gov/1201/.

As such, any mechanisms manufacturers attempt to employ in order to prevent end-user modification of the software running on their RF-enabled devices is likely to be easily bypassed by technologically competent end-users. And since such end-users already make up the bulk of individuals performing modifications to such software, it is unlikely that the proposed rules will actually be effective in decreasing the number of end-users modifying the software on their devices. It follows that any interference or other issues related to such modifications are unlikely to be effectively resolved by the proposed rules.

3. Alternative solutions for reducing harmful interference resulting from the end-user modification of RF-enabled devices.

While the proposed rules would be harmful to end-users and ineffective at resolving interference problems, there are efforts the Commission can undertake to reduce potential problems with allowing end-user modification of the software on RF-enabled devices.

A. It is not clear that end-user modification of software on RF-enabled devices is a common cause of harmful RF interference.

Generally, the biggest concern raised with allowing end-users to modify the software on their RF-enabled devices is that such modification might allow the device to operate in a manner that causes harmful interference to other spectrum users. Perhaps the most pressing example of these kinds of issues relate to the interference 5 GHz-capable U-NII WiFi devices can cause on Terminal-area Doppler Weather Radar (TDWR) systems.[13] Such interference can occur if users utilize unapproved 5 GHz channels or if they use devices that do not properly implement Dynamic Frequency Selection (DFS).[14] The NTIA

[13] Matthew Gast, *Why we lost the weather radar channels,* Boundless, February 7th, 2013.
[14] WIFI Insider, *Dynamic Frequency Selection,* accessed on October 8th, 2015, http://wifi-insider.com/wlan/dfs.htm.

has undertaken a multi-part case-study of this issue and the Commission has undertaken a number of enforcement actions in response to such interference.[15]

It appears, however, that in most, if not all of these cases, the harmful interference did not result due to the end-user modification of otherwise approved devices, but from the use of devices that were either unapproved by the Commission, flawed in their design, or on which DFS was not enabled.[16] Indeed, it is difficult to find evidence that end-user modifications are significantly contributing to the kinds of interference events with which the Commission is most concerned. If the end-user modification of RF device software is not a significant cause of harmful interference, it would seem unjustified to introduce mandates aimed at preventing such modifications given the previously outlined harms such mandates could cause.

B. The Commission should seek to work with third-party RF-enabled device software communities to ensure compliance.

Assuming, arguendo, that the end-user modification of the software on RF-enabled devices is a significant source of harmful interference, the Commission should work with the developers and users of such software to resolve these issues directly.

---

[15] National Telecommunications and Information Administration (NTIA), *Technical Report TR-11-473 - Case Study: Investigation of Interference into 5 GHz Weather Radars from Unlicensed National Information Infrastructure Devices, Part I,* Department of Commerce, November 2010; NTIA, *Technical Report TR-11-479 - Case Study: Investigation of Interference into 5 GHz Weather Radars from Unlicensed National Information Infrastructure Devices, Part II,* Department of Commerce, July 2011; NTIA, *Technical Report TR-12-486 - Case Study: Investigation of Interference into 5 GHz Weather Radars from Unlicensed National Information Infrastructure Devices, Part III,* Department of Commerce, June 2012; US FCC, *Weather Radar Interference Enforcement,* accessed on October 8th, 2015, https://www.fcc.gov/encyclopedia/weather-radar-interference-enforcement.

[16] NTIA, TR-11-473, 15-23.

Linux-based RF-device software projects already strive to ensure their software complies with the requirements of both the Commission and other regulatory bodies around the world. Software subsystems such as the Linux Central Regulatory Domain Agent (CRDA) exist for the sole purpose of ensuring that Linux-based RF-device software operates in a manner consistent with the regulations applicable to a given region.[17] Such software limits the channels, power, and modes of operation available to the end-user and is included in OpenWRT and other major RF-device software projects.[18] If there are deficiencies in such software that are leading to unintentional instances of harmful interference, they can be corrected via fixes to the software itself.

In some cases, interface problems might be best corrected by ensuring that RF-enabled device software ships with suitable values chosen for the default configuration. Such "complaint by default" configurations can help ensure that users of such software do not unintentionally cause harmful interference. For example, OpenWRT currently ships with DFS support disabled by default.[19] This is a flaw that can and should be corrected by the OpenWRT community — either by enabling DFS by default or by removing support for channels that require DFS unless it is explicitly enabled. The Commission could engage with such communities to request that they fix such flaws and to ensure that default configuration shipped with their software meets the necessary regulatory requirements.

---

[17] Linux Wireless, *Central Regulatory Domain Agent*, kernel.org, accessed October 8th, 2015, https://wireless.wiki.kernel.org/en/developers/regulatory/crda.
[18] OpenWRT, *OpenWRT Wireless FAQ: Regulation in law*, accessed on October 8th, 2015, http://wiki.openwrt.org/doc/faq/faq.wireless.
[19] OpenWRT, "Wireless configuration: DFS/Radar Detection," accessed on October 8th, 2015, http://wiki.openwrt.org/doc/uci/wireless.

The Commission could also work with end-users within such communities to educate them on the importance of ensuring regulatory compliance when using RD-enabled device software. It is unlikely that the majority of the members of such communities are intentionally subverting Commission rules; such an outreach effort would likely be highly effective in reducing instances of unintentional misuse of RF-devices.

The ability and willingness of the Commission to engage with members and developers in the communities providing alternative software implementations for RF-enabled devices would go a long way toward reducing potential RF interference violations caused by such software. Such efforts will likely be far more effective at reducing harmful interference than merely attempting to lock out end-user modifications.

C. End-users or others modifying RF-enabled equipment for the purpose of causing harmful interference or otherwise violating Commission rules should be dealt with on a case-by-case enforcement basis.

End-users or others who are intentionally attempting to cause harmful interference or who are acting in a reckless manner resulting in such interference should be dealt with via target enforcement actions. Indeed, this is how the Commission has historically dealt with end-users employing modified or unmodified hardware in a non-compliant manner.[20] For example, the Commission never attempted to require the manufacturers of analog radio hardware to attempt to make it impossible for end-users to modify such hardware by replacing individual electronic components. The fact that modern hardware is more often controlled by software components than by electronic components does not necessitate a new approach to enforcement.

[20] FCC, *Weather Radar Interference Enforcement*.

4. Conclusion

The Commission should refrain from implementing the rules as proposed or any rules that will reduce the ability of end-users to modify and control the software running on their RF-enabled devices. Instead, the Commission should seek to work with the communities developing and deploying such software to ensure the software operates within the legal parameters and to pursue targeted enforcement action against specific bad actors. These approaches will be both more effective and less harmful than the proposed rules.

To the extent that the Commission wishes to further explore the nuances of regulating and preventing harmful interference caused by software-controlled RF-devices, such a discussion would be best relegated to a dedicated proceeding. This is an important topics with far reaching implications, and as such deserves a dedicated proceeding in which the Commission solicits feedback from all concerned stakeholders. Rules related to the limitation or control of software modifications on RF-enabled devices should thus be removed from the current proceeding, and either dropped in favor of the alternate solution suggested herein, or re-addressed via a separate dedicated proceeding.

Respectfully submitted,

Mr. Andy Sayler
Mr. Matt Monaco
Prof. Dirk Grunwald, Ph.D.
University of Colorado, Boulder
Department of Computer Science
Contact: andy.sayler@colorado.edu
October 9, 2015